



제429회국회(정기회)
제6차기획재정위원회

조세특례제한법 일부개정법률안

검 토 보 고

■ 이해민의원 대표발의(의안번호 제11163호)

2025. 11.

기 획 재 정 위 원 회

전문위원 정지은

목 차

I . 개요	1
II . 주요 내용별 검토	3
1. .정보보호 관련 세액공제 신설(이해민의원안)	3

I. 개요

1. 이해민의원 대표발의안(의안번호 제11163호)

가. 제안경위

- (1) 제 안 자 : 이해민의원 등 10인
- (2) 제 안 일 : 2025. 6. 30.
- (3) 회 부 일 : 2025. 7. 1.

나. 제안이유 및 주요내용

AI 시대가 도래함에 따라 개인정보의 활용과 처리 속도가 비약적으로 증대되면서, 기업에 대한 사이버 침해가 초래할 수 있는 피해 역시 과거보다 훨씬 심각해지고 있음. 특히 최근 발생한 SKT의 사이버침해 사고 및 유심정보유출 사건으로 국내 기업 전반의 정보보호 수준을 점검하고 정보보호 관련 역량을 강화할 필요가 있다는 의견이 제기되고 있음.

그러나 여전히 많은 기업들이 최소한의 법적 기준만을 지키며 추가적인 정보보호 투자에는 소극적인 태도를 보이고 있어 정보보호 역량 강화를 위한 실질적이고 지속적인 유인책이 마련될 필요가 있음.

특히 중소기업의 경우 상대적으로 정보보호 관련 인력과 자원이 부족하고, 관련 투자비용에 대한 부담이 크기 때문에 실효성 있는 지원 방안이 마련될 필요가 있다는 의견이 제기됨.

이에 따라 정보보호 시스템설비 투자비용, 정보보호 컨설팅 비용 및 정보보호 관련 보험 가입비용에 대한 세액공제를 마련하고, 정보보호 전문인력을 신규채용 시 세액공제를 하도록 하여 정보보호와 관련된 투자 및 인력 채용을 지원하려는 것임(안 제24조제1항제2호가목, 안 제104조의36 및 제104조의37 신설).

II. 주요 내용별 검토

1. 정보보호 관련 세액공제 신설(이해민의원안)

현행	개정안																													
○ <신설>	○ 정보보호 시스템설비 통합투자세액공제율 상향(안 제24조) ○ 공제대상: 기계장치 등 사업용 유형자산, 그 외 대통령령으로 정하는 유형자산과 무형자산에 투자하는 경우 해당 투자금액 ○ 유형별 공제율 <table><tr><th rowspan="2">구분(%)</th><th colspan="3">기본</th><th rowspan="2">추가*</th></tr><tr><th>대</th><th>중견</th><th>중소</th></tr><tr><td>일반</td><td>1</td><td>5, 7.5¹⁾</td><td>10</td><td rowspan="5">10</td></tr><tr><td>신성장원천기술 사업화시설 및 연구개발시설</td><td>3</td><td>6, 9²⁾</td><td>12</td></tr><tr><td>국가전략기술 사업화시설 및 연구개발시설</td><td>15</td><td>15, 20³⁾</td><td>25</td></tr><tr><td>반도체 분야</td><td>20</td><td>20, 25⁴⁾</td><td>30</td></tr><tr><td>정보보호 시스템설비**</td><td>15</td><td>15, 20³⁾</td><td>25</td></tr></table> * (당해연도 투자액 - 직전 3년 평균 투자액) ** 「정보보호산업의 진흥에 관한 법률」 제2조제1항제1호에 따른 정보보호 시스템에 사용되는 설비로서 대통령령으로 정하는 설비 1) (~3년)7.5%, (4년~)5% 2) (~3년)9%, (4년~)6% 3) (~3년)20%, (4년~)25% 4) (~3년)25%, (4년~)20% ○ 적용기한: 없음 ○ 시행일: 2026. 1. 1. ○ 적용례: 이 법 시행 이후 투자하는 경우부터 적용	구분(%)	기본			추가*	대	중견	중소	일반	1	5, 7.5 ¹⁾	10	10	신성장원천기술 사업화시설 및 연구개발시설	3	6, 9 ²⁾	12	국가전략기술 사업화시설 및 연구개발시설	15	15, 20 ³⁾	25	반도체 분야	20	20, 25 ⁴⁾	30	정보보호 시스템설비**	15	15, 20 ³⁾	25
구분(%)	기본			추가*																										
	대	중견	중소																											
일반	1	5, 7.5 ¹⁾	10	10																										
신성장원천기술 사업화시설 및 연구개발시설	3	6, 9 ²⁾	12																											
국가전략기술 사업화시설 및 연구개발시설	15	15, 20 ³⁾	25																											
반도체 분야	20	20, 25 ⁴⁾	30																											
정보보호 시스템설비**	15	15, 20 ³⁾	25																											
○ <신설>	○ 정보보호비용 세액공제 신설(안 제104조의36 신설) ○ 공제대상: 내국인이 정보보호를 위하여 ①정보통신시설 및 시스템을 안전하게 유지하기 위한 보호대책 수립, 위험요인평가, 모의해킹, 마스터플랜 수립 등을 수행하는 업무용역을 이용하기 위하여 정보보호 전문서비스 기업 등에 지출한 비용과 ② 해킹 등 정보통신망 등을 공격하는 행위로 발생한 침해사고로 인하여 발생하는 손해를 보상하기																													

현 행	개정안
○ <신 설>	위한 보험상품에 가입하여 해당 과세연도에 납입한 보험료 납부액(의무가입 상품 제외) ○ 공제율: 대기업 1%, 중견기업 3%, 중소기업 5% ○ 공제한도: 해당 과세연도 소득세 또는 법인세의 10% ○ 적용기한: 2028. 12. 31. ○ 시행일: 2026. 1. 1. ○ 적용례: 이 법 시행 이후 정보보호비용을 지출하는 경우부터 적용 ○ 정보보호 전문인력 고용기업 세액공제(안 제104조의37 신설) ○ 공제대상: 내국인이 정보보호 전문인력*을 고용하는 경우 고용인원 1인당 대기업 400만원, 중견기업 600만원, 중소기업 1,000만원씩 공제 * ①「정보보호산업의 진흥에 관한 법률」 제2조제1항제1호에 따른 정보보호와 관련하여 대통령령으로 정하는 자격기준을 갖춘 기술인력일 것, ②정보보호 전담인력으로 정보보호 관련 업무를 수행할 것, ③해당 기업의 최대주주 또는 최대출자자나 그와 대통령령으로 정하는 특수관계에 있는 사람이 아닐 것 ○ 공제 이후 1년 이내 근로관계 종료 시 사후추징 ○ 통합고용세액공제와 중복적용 배제 ○ 적용기한: 2028. 12. 31. ○ 시행일: 2026. 1. 1. ○ 적용례: 이 법 시행 이후 정보보호 전문인력을 고용하는 경우부터 적용

* 이해민의원안 2025. 6. 30. 발의(의안번호 11163)

□ 개정안은 국내 기업의 정보보호 역량 강화를 위한 실질적인 유인책을 마련하기 위하여 정보보호 시스템설비 통합투자세액공제율 상향, 정보보호비용 세액공제 신설, 정보보호 전문인력 고용 시 세액공제 적용 등 정보보호를 위하여 지출하는 비용에 대하여 세제혜택을 부여하려는 것임.

먼저 현행법상 내국인이 「정보보호산업의 진흥에 관한 법률」 제2조제1항제1호에 따른 정보보호시스템¹⁾에 사용되는 설비로서 대통령령으로 정하는 설비에 투자하는 경우 이는 일반적인 사업용 유형자산에 대한 투자로 분류되어 투자금액에 대하여 1%~10%의 기본공제율이 적용되는데, 안 제24조는 이에 대하여 국가전략기술 사업화 시설 및 연구개발시설과 동일하게 15%~25%의 상향된 기본공제율을 적용하도록 하려는 것임.

[통합투자세액공제 유형별 공제율]

(단위: %)

구 분	기본공제			추가공제 ^{주)}
	대	중견	중소	
일 반 (현행)	1	5, 7.5 ¹⁾	10	10
신성장·원천기술 사업화시설 및 연구개발시설	3	6, 9 ²⁾	12	
국가전략기술 사업화시설 및 연구개발시설	15	15, 20 ³⁾	25	
반도체 분야	20	20, 25 ⁴⁾	30	
정보보호 시스템설비 (개정안)	15	15, 20 ³⁾	25	

주) 추가분=당해연도 투자액 - 직전 3년 평균 투자액

1) (~3년)7.5%, (4년~)5%

2) (~3년)9%, (4년~)6%

3) (~3년)20%, (4년~)15%

4) (~3년)25%, (4년~)20%

1) 「정보보호산업의 진흥에 관한 법률」

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보보호”란 다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 “정보보호시스템”이라 한다)을 마련하는 것을 말한다.

가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것

나. 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것

다음으로 안 제104조의36은 내국인이 정보보호를 위해 ①정보통신 시설 및 시스템을 안전하게 유지하기 위한 보호대책 수립, 위험요인 평가, 모의해킹, 마스터플랜 수립 등을 수행하는 업무용역을 이용하기 위하여 「정보보호산업의 진흥에 관한 법률」 제23조에 따른 정보 보호 전문서비스 기업²⁾ 및 대통령령으로 정하는 이에 준하는 기관

2) 「정보보호산업의 진흥에 관한 법률」

제23조(정보보호 전문서비스 기업의 지정·관리) ① 과학기술정보통신부장관은 다음 각 호의 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 정보보호 전문서비스 기업으로 지정할 수 있다.

1. 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설(이하 이 조에서 “주요정보통신기반시설”이라 한다)의 취약점 분석·평가 업무
2. 주요정보통신기반시설 보호대책의 수립 업무
3. 그 밖에 정보보호서비스와 관련하여 대통령령으로 정하는 업무

② 정보보호 전문서비스 기업으로 지정받을 수 있는 자는 법인으로 한다.

③ 과학기술정보통신부장관은 제1항에 따라 지정된 정보보호 전문서비스 기업에 대하여 지정일 부터 매 1년마다 사후관리 심사를 수행하여야 한다.

④ 정보보호 전문서비스 기업은 업무를 양도하거나 다른 정보보호 전문서비스 기업과 합병하는 경우에는 과학기술정보통신부장관에게 신고하여야 한다. 이 경우 양수인 또는 합병된 법인은 과학기술정보통신부장관이 신고를 수리한 때에 정보보호 전문서비스 기업의 지위를 승계한다.

⑤ 정보보호 전문서비스 기업이 휴업·폐업하거나 업무를 재개할 때에는 휴업·폐업하려는 날 또는 휴업 후 업무를 재개하려는 날의 30일 전까지 과학기술정보통신부장관에게 신고하여야 한다.

⑥ 과학기술정보통신부장관은 정보보호 전문서비스 기업이 다음 각 호의 어느 하나에 해당하는 경우에는 청문을 거쳐 정보보호 전문서비스 기업의 지정을 취소하거나 3개월 이내의 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호, 제2호, 제4호의 어느 하나에 해당하는 경우에는 지정을 취소하여야 한다.

1. 속임수나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 제3항에 따른 사후관리 심사를 통과하지 못한 경우
3. 제8항을 위반하여 기록 및 자료를 안전하게 보존하지 아니한 경우
4. 제10항에 따른 지정기준에 미달한 경우
5. 업무를 수행하면서 알게 된 정보를 오·남용하여 주요정보통신기반시설의 운영에 장애를 가 저은 경우

⑦ 과학기술정보통신부장관은 정보보호를 위하여 특히 필요하다고 인정하는 경우에는 정보보호 전문서비스 기업으로 하여금 관련 서류 또는 자료를 제출하게 할 수 있다. <개정 2017. 7. 26.>

⑧ 정보보호 전문서비스 기업은 제1항 각 호의 업무와 관련하여 작성한 기록 및 자료를 안전하게 보존하여야 한다.

⑨ 정보보호 전문서비스 기업은 제1항에 따른 지정이 취소되거나 폐업한 때에는 제1항 각 호의 업무와 관련한 기록 및 자료를 해당 기관 또는 기업의 장에게 반환하거나 폐기하여야 하며, 반환이 곤란하거나 불가능한 자료에 대해서는 폐기할 자료를 특정하여 해당 기관 또는 기업의 장의 승인을 얻은 후 폐기하여야 한다.

⑩ 제1항에 따른 지정, 제3항에 따른 사후관리 심사, 제4항에 따른 양도·합병, 제5항에 따른 휴업 등의 신고, 제6항에 따른 지정취소, 제7항에 따른 자료제출, 제9항에 따른 기록 및 자료의 반환, 폐기의 절차 및 방법 등에 관하여 필요한 사항은 과학기술정보통신부령으로 정한다.

에 지출한 비용과 ②기업을 피보험자로 하는 보험상품 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고³⁾로 인하여 발생하는 손해를 보상하기 위한 보험상품에 가입하여 해당 과세연도에 납입한 보험료 납부액의 합계액(「개인정보 보호법」 제39조의7⁴⁾에 따라 가입한 손해배상책임의 이행을 위한 보험 등 법령에 따라 의무적으로 가입한 보험에 해당하는 보험료 납부액은 제외) 등 정보보호비용을 지출하는 경우 대기업 1%, 중견기업 3%, 중소기업 5%의 공제율을 적용하려는 것임.

마지막으로 안 제104조의37은 내국인이 ①정보보호와 관련하여 대통령령으로 정하는 자격기준을 갖춘 기술인력을 고용하여 정보보호 전담인력으로 정보보호 관련 업무를 수행하도록 할 경우 고용 인원 1인당 대기업 400만원, 중견기업 600만원, 중소기업 1,000만원 씩 고용이 발생한 날이 속하는 과세연도에 세액공제 혜택을 부여하려는 것임.

□ 2025년 4월 18일 SK텔레콤은 평소 대비 대용량 데이터가 외부로 전송된 상황을 인지하고 4월 20일 한국인터넷진흥원에 침해사고를 신

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

7. “침해사고”란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

4) 「개인정보 보호법」

제39조의7(손해배상의 보장) ① 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.

고하였음.

과학기술정보통신부에 따르면 2025년 4월 SK텔레콤 침해사고에 따라 유출된 정보는 전화번호, 가입자 식별번호(IMSI: International Mobile Subscriber Identity) 등 유심정보 25종이고 유출규모는 9.82GB, IMSI 기준 약 2,696만건임.

SK텔레콤 침해사고 민관합동조사단은 계정정보 관리 부실, 과거 침해사고 대응 미흡, 주요 정보 암호화조치 미흡 등을 사고의 원인으로 지적하였고, 유사 사고 재발 방지를 위하여 비밀번호 관리 강화, 주요 정보 암호화, 정보보호 관리체계 강화, 정보보호 인력 및 예산 확대 등을 대책으로 제시하였음.

- 개정안은 SK텔레콤 침해사고와 같은 사고가 재발하지 않도록 사전에 국내 기업의 정보보호 수준을 점검하고 관련 역량을 강화하기 위하여 정보보호 관련 투자에 대한 세제 측면의 유인책을 마련하려는 것으로, 다음과 같은 점에서 필요한 측면이 있어 보임.

첫째, SK텔레콤 침해사고 민관합동조사단이 “타사 대비 정보보호 인력 및 투자 규모 부족”을 침해사고의 원인 중 하나로 지적하였다는 점을 감안할 때, 침해사고를 예방하기 위하여 개인정보를 취급하는 기업으로 하여금 정보보호 인력 확충 및 투자 확대를 유도할 필요성이 있어 보임.

2024년도 정보보호 공시 기준 SK텔레콤의 가입자 100만명당 정보보호 인력은 15.0명, 투자액은 37.9억원으로 통신사 평균에 비해 그

규모가 작았고, 이에 민관합동조사단은 SK텔레콤으로 하여금 정보 보호 강화에 필요한 인력 및 예산규모를 타 통신사 이상의 수준으로 확대할 것을 재발방지 대책으로 제시한 바 있음.

[가입자 100만명 당 정보보호 인력 및 투자액]

(단위: 명, 억원)

구 분	SK텔레콤	KT	LGU+	평균
가입자 100만명 당 정보보호 인력	15.0	25.1	14.3	17.7
가입자 100만명 당 정보보호 투자액	37.9	90.8	57.5	57.4

자료: 과학기술정보통신부 보도자료, 2025. 7.

둘째, 침해사고가 발생할 경우 수반되는 사회적 비용이 크다는 점을 고려할 필요가 있음.

2020년 사이버 침해사고로 인한 국내 기업부문 연간 피해액은 사고 조사, 대응, 복구 등 직접비용과 예방비용 및 기업 가치손실 등 간접비용을 합산한 결과 약 6,956억원으로 추정되었고, 시간 손실, 정신적 피해 등 개인의 피해비용을 산출한 결과 약 9,834억원의 비용이 발생한 것으로 나타났음.⁵⁾

또한, 침해사고로 유출된 개인정보는 금융정보 탈취, 신원 도용과 같은 2차 피해로 이어질 수 있음.⁶⁾

□ 다만, 개정안과 관련하여 다음과 같은 측면을 감안할 필요가 있어 보임.

5) 한국인터넷진흥원, “사이버 침해사고의 경제·사회적 비용 추정 연구”, 2021. 12.

6) 2021년 미국 이동통신사 T-Mobile이 해킹되어 약 4천만 명 이상의 성명, 생년월일, 사회보장번호, 운전면허증 정보 등이 유출되고 그 중 1,310만명은 IMSI, IMEI 정보까지 유출되었는데, 일부 피해자들이 유출된 정보를 이용한 피싱 문자를 받는 등의 피해를 겪은 것으로 보고되었음. (출처: 국회입법조사처, “통신사 해킹 사고 사후대응의 문제점과 입법과제”, 2025. 5.)

첫째, 고객의 정보를 보호하는 것은 기업의 기본적인 책무로서 세제지원 등 정부가 지원할 분야에 해당한다고 보기 어려운 측면이 있음.

기획재정부는 정보보호에 대한 세제 인센티브를 부여하기보다 정보 유출에 대한 손해배상 강화 및 기업의 의무지출 확대 등 직접적인 규제가 필요하다는 의견을 제시함.

둘째, 정보보호 시스템설비 투자비용에 대해 일반적인 사업용 유형자산보다 높은 공제율을 적용하는 것은 통합투자세액공제(법 제24조)를 도입한 취지에 부합하지 않는 측면이 있음.

통합투자세액공제는 기존에 존재하던 중소기업등 투자세액공제, 특정시설 투자세액공제⁷⁾, 의약품 품질관리개선시설 투자세액공제 등을 하나의 제도로 통합하여 모든 사업용 유형자산에 대해 동일하게 공제를 적용하기 위해 2020년 세법개정을 통해 신설되었음.

다만, 미래 유망성 및 산업 경쟁력 등을 고려하여 지원할 필요성이 인정되는 신성장·원천기술과 국가안보 차원의 전략적 중요성이 인정되고 국민경제 전반에 중대한 영향을 미치는 국가전략기술에 한하여 일반적인 투자 대비 높은 공제율을 적용하고 있음.

통합투자세액공제의 도입 취지 및 공제율 적용구조를 고려할 때 정보보호 시스템설비 투자비용에 대하여 국가전략기술 사업화시설 및 연구개발시설 투자비용과 동일한 공제율을 적용하는 것은 투자

7) 연구시험용 및 직업 훈련용 시설, 에너지절약시설, 환경보전시설, 근로자복지증진시설, 안전시설, 생산성향상시설 등이 특정시설 투자세액공제 대상에 포함되었음.

에 대한 현행 세제지원 체계와는 방향성이 맞지 않는 측면이 있음.
셋째, 기업이 이윤 극대화를 목표로 자율적으로 가입을 결정한 보험료 등에 대해 조세지출을 확대해 지원하는 것이 정당한지에 대한 논의가 필요함.

정보보호 시스템 구축 및 관련 투자 증대는 침해사고 발생 시 복구비용, 기업 신뢰도 하락 등 다양한 잠재적 비용을 기업 스스로 고려하여 내리는 경영적 판단이며, 그에 따른 책임 역시 전적으로 해당 기업에 귀속된다고 보는 것이 타당함.

참고로 현재 기업이 부담하는 보험료에 대해 세액감면이나 공제 혜택 등 조세특례를 적용하는 입법례는 없음.

넷째, 정보보호 전문인력을 고용한 기업에 대한 세액공제(안 제104조의37)의 경우 제도 시행을 위해 일부 보완조치가 필요해 보임.

개정안에 따르면 내국인이 정보보호와 관련하여 대통령령으로 정하는 자격기준을 갖춘 인력을 고용하여 해당 인력으로 하여금 정보보호 관련 업무를 수행하도록 할 경우 고용 인원 1인당 400만원 ~1,000만원의 세액공제 혜택을 적용받을 수 있음.

다만, 정보보호 관련 자격증을 갖춘 자를 고용한 이후 해당 인력이 정보보호 관련 업무를 실제로 수행하는지에 대한 검증이 현실적으로 어려울 것으로 보임.

또한, 개정안은 정보보호 전문인력을 신규 채용하는 경우에 한하여

공제혜택을 적용하도록 규정하고 있는데,⁸⁾ 이는 기존에 정보보호 인력을 고용하고 있는 기업에 대한 차별적인 조치에 해당함.

문 의 처

02)6788-5154

8) 안 부칙 제4조(정보보호 전문인력을 고용한 기업에 대한 세액공제에 관한 적용례) 제104조의37의 개정규정은 이 법 시행 이후 정보보호 전문인력을 고용하는 경우부터 적용한다.